Patent number: DE3313098
Publication date: 1984-10-11
Inventor: KURTH HERMANN DIPL-ING; KRUEGENER ROLF DIPL-ING
Applicant: DAIMLER BENZ AG
Classification:
- international: E05B49/00
- european: G07C9/00B12; G07C9/00E4
Application number: DE19833313098 19830412
Priority number(s): DE19833313098 19830412

Also published as:
F R2544368 (A1)
IT117 3488 (B)

Abstract of **DE3313098**

What is described is a falsification-proof electronic lock system which consists of an electronic key and a lock control. According to the invention, a dialogue based on question-and-answer code signals is conducted between these two modules, an actuation of the bolt of the lock becoming possible only after a respective parts dialogue has been acknowledged.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(11) **DE 3313098 C1**

(51) Int. Cl. 3: E05B 49/00

(21) Aktenzeichen: P 33 13 098.1-31
(22) Anmeldetag: 12. 4. 83
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 11. 10. 84

DE 3313098 C1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:

Daimler-Benz AG, 7000 Stuttgart, DE

(72) Erfinder:

Kurth, Hermann, Dipl.-Ing.; Krügener, Rolf, Dipl.-Ing., 7032 Sindelfingen, DE

(56) Im Prüfungsverfahren entgegengehaltene Druckschriften nach § 44 PatG:

DE-OS 30 06 128
EP-OS 00 68 437

(54) Elektronisches Schloßsystem

Es wird ein fälschungssicheres elektronisches Schloßsystem beschrieben, welches aus einem elektronischen Schlüssel und einer Schloßsteuerung besteht. Erfindungsgemäß wird zwischen diesen beiden Bausteinen ein Dialog auf Basis von Frage- und Antwort-Codesignalen geführt, wobei eine Riegelbetätigung des Schlosses nur nach jeweils bestätigtem Teildialog ermöglicht wird.

DE 3313098 C1

Patentansprüche:

1. Elektronisches Schloßsystem, insbesondere für Kraftfahrzeuge, umfassend einerseits einen elektronischen Schlüssel mit einem Speicher und einem Öffnungscodesignale abgebenden Sender und andererseits eine Schloßsteuerung mit einem das empfangende Öffnungscodesignal mit einem in einem Fest- und Lesespeicher gespeicherten Codesignal vergleichenden Codevergleicher, welche bei Übereinstimmung der beiden Codesignale ein Schaltsignal erzeugt und ferner mit einem Zufallscodesignale erzeugenden Zufallsgenerator, dessen Zufallscodesignale den Speicher des elektronischen Schlüssels aktivieren, dadurch gekennzeichnet, daß das Schaltsignal den Fest- und Lesespeicher (11) der Schloßsteuerung (3) zur Abgabe von Fragecode (19) an den Zufallsgenerator (16) aktiviert, dieser (16) die Fragecode (19) gemischt als Zufallscodesignale (20) an den elektronischen Schlüssel (2) aussendet, welcher (2) über einen Codevergleicher (6) im Speicher (5) gespeicherte Antwortcode (21) mit den als Zufallscodesignale (20) empfangenen Fragecode (19) vergleicht und bei Bestätigung der beiden Code (21; 19, 20) über den Sender (4) ein Antwortcodesignal (22) an den Empfänger (10) der Schloßsteuerung (3) aussendet, deren Codevergleicher (12) und Datenauswerter (13) das ausgesendete und in den Lesespeicher (11) eingeschriebene Zufallscodesignal (20) mit dem Antwortcodesignal (22) vergleicht und auswertet und bei Bestätigung von dieser (3) ein Signal (23) zur Riegelbetätigung des Schlosses (17) abgegeben wird.

2. Elektronisches Schloßsystem nach Anspruch 1, dadurch gekennzeichnet, daß die Schloßsteuerung (3) einen Zähler- und Zeitschalter (14) aufweist, welcher bei fehlendem oder falschem Antwortcodesignal (22) aktiviert wird und das Schaltsignal zur Abgabe von Fragecode (19) aus dem Fest- und Lesespeicher (11) verzögert.

3. Elektronisches Schloßsystem nach Anspruch 1 und 2, dadurch gekennzeichnet, daß der Zähler- und Zeitschalter (14) bei häufigen Öffnungscodesignalempfängen pro kurzer Zeiteinheit aktiviert wird und ein Verweigerungsglied (15) der Schloßsteuerung (3) aktiviert.

4. Elektronisches Schloßsystem nach Anspruch 1 und 3, dadurch gekennzeichnet, daß das Verweigerungsglied (15) durch ein separates Entsperrcodesignal (24) vom Sender (4) inaktivierbar ist.

Die Erfindung betrifft ein elektronisches Schloßsystem gemäß dem Oberbegriff des Anspruches 1.

Es ist ein schlüsselloses, elektronisches Schloßsystem für Kraftfahrzeuge bekannt (EP-OS 00 68 437), bei welchem durch Eingabe eines Code über eine außen an der Fahrzeugtür angebrachte, digitale Druckknopftastatur der Türschließmechanismus entriegelt werden kann. Um eine hohe Fälschungssicherheit zu erreichen, werden in diesem Schloßsystem zwei Code verwendet und zwar ein fest eingespeicherter, nicht veränderbarer und nur dem Fahrzeugbesitzer bekannter erster Code und ein vom Fahrzeugbesitzer variierbarer, eine hohe Anzahl von Codiervarianten zulassender zweiter Code.

Zum Öffnen des Schloßsystems ist hierbei nur der zweite Code erforderlich, welcher jedoch nach Bedarf manuell dadurch geändert werden kann, daß nach Eingabe des ersten Code der beliebig gewählte zweite Code eingegeben und in dessen Speicher eingeschrieben werden kann und somit beim nächsten Öffnungsvorgang das Schloßsystem nur mit diesem neuen variierten zweiten Code aktivierbar ist. Da eine hohe Anzahl von Codiervarianten nur mit einer entsprechenden Anzahl von Drucktasten erzielbar ist, ist es für den Benutzer unerläßlich, sich stets die Ziffern-Code-Kombination zu merken. Dies dürfte in der Praxis zu erheblichen Schwierigkeiten führen.

Desweiteren ist aus der DE-OS 30 06 128 ein gattungsgemäßes Schloßsystem bekannt. Bei diesem ebenfalls eine hohe Anzahl möglicher Codiervarianten und somit eine hohe Fälschungssicherheit erreichenden Schloßsystem wird der Speicher des elektronischen Schlüssels über eine Vielzahl elektrischer Kontakte an dem Schlüssel mit der Schloßsteuerung verbunden. Die Schloßsteuerung vergleicht das empfangene und aus dem Speicher des Schlüssels ausgesendete Codesignal mit einem schloßseitig vorgegebenen Signal. Wenn das in dem Fest- und Lesespeicher der Schloßsteuerung gespeicherte Signal mit dem empfangenen Codesignal übereinstimmt, erzeugt die Schloßsteuerung ein Schaltsignal, welches das Schloß öffnet. Beim Schließvorgang hingegen verbindet die Schloßsteuerung bei Übereinstimmung der Signale einen Zufallsgenerator mit den Speichern des elektronischen Schlüssels und der Schloßsteuerung, wobei die vom Zufallsgenerator erzeugten Codesignale in die Speicher eingeschrieben werden, so daß erst nach dem Einschreiben von der Schloßsteuerung ein Schaltsignal erzeugt wird, welches das Schloß schließt. Auf diese Weise wird also das Schlüsselgeheimnis selbsttätig während jedes Schließvorganges der Schloßsteuerung geändert, wodurch aber das Schloßsystem lediglich mit dem beim unmittelbar vorhergehenden Schließvorgang benutzten Schlüssel betätigt werden kann.

Aufgabe der Erfindung ist es, ein gattungsgemäßes Schloßsystem auf einem anderen Wege so auszubilden, daß es ebenfalls eine hohe Fälschungssicherheit erreicht, gleichwohl aber von mehreren identischen Schlüsseln betätigt werden kann.

Diese Aufgabe wird erfindungsgemäß durch die kennzeichnenden Merkmale des Anspruches 1 gelöst.

Hierdurch wird erreicht, daß das Schloßsystem von mehreren identischen Schlüsseln betätigt werden kann, sofern diese in ihrem Speicher jeweils mit den gleichen Öffnungs- und Antwortcode programmiert sind. Die hohe Fälschungssicherheit ist dadurch gegeben, als der Dialog-Code zwischen elektronischem Schlüssel und Schloßsteuerung durch die Zwischenschaltung des Zufallsgenerators laufend geändert wird, so daß eine Benutzung des aufgezeichneten Dialoges von und durch einen Unbefugten nicht zum Entriegeln der Tür führt.

Anhand eines Ausführungsbeispiels wird die Erfindung näher beschrieben. Die Zeichnung stellt ein schematisches Blockschaltbild des aus elektronischem Schlüssel und Schloßsteuerung bestehenden Schloßsystems dar.

Das elektronische Schloßsystem 1 umfaßt einen elektronischen Schlüssel 2 und eine Schloßsteuerung 3, wobei der elektronische Schlüssel 2 im wesentlichen einen Sender 4, Speicher 5, Codevergleicher 6 und eine Datensteuerung 7 mit Datenausgabe 8 und die Schloßsteuerung 3 einen elektronischen Baustein 9 — enthaltend

einen Empfänger 10, einen Fest- und Lesespeicher 11, einen Codevergleicher 12, einen Datenauswerter 13, einen Zähler- und Zeitschalter 14 und ein Verweigerungsglied 15 — und einen Zufallsgenerator 16 enthält. Sämtliche Bauteile sind in der erforderlichen funktionellen Weise miteinander verschaltet.

Soll nun beispielsweise das Schloß 17 der Kraftfahrzeugtür entriegelt werden, so wird vom elektrischen Schlüssel 2 über dessen Sender 4 ein im Speicher 5 fest programmiertes Öffnungscodesignal 18, z. B. als Infrarot-, Ultraschall- oder Funksignal, an den Empfänger 10 der Schloßsteuerung 3 ausgesendet. Deren Codevergleicher 12 vergleicht das empfangene Öffnungscodesignal 18 mit einem in dem Fest- und Lesespeicher 11 fest gespeicherten Codesignal. Stimmen die beiden Codesignale überein, so wird von dem Datenauswerter 13 ein Schaltsignal erzeugt, welches den Fest- und Lesespeicher 11 zur Abgabe von fest gespeicherten Fragecode 19 an den Zufallsgenerator 16 aktiviert. Dieser mischt die Fragecode 19 willkürlich und sendet diese als Zufallscodesignal 20 zum einen an den elektronischen Schlüssel 2 und zum anderen an den elektronischen Baustein 9 aus, wo es in den Lesespeicher 11 eingeschrieben wird. Das vom elektronischen Schlüssel 2 empfangene Zufallscodesignal 20 wird in dessen Codevergleicher 6 mit im Speicher 5 fest programmierten Antwortcode 21 verglichen — der Speicher 5 enthält zu jedem Zufallscodesignal 20 einen genau definierten Antwortcode 21 —, wobei bei Bestätigung der beiden Code über die Datensteuerung 7 und Datenausgabe 8 der Sender 4 zur Aussendung eines Antwortcodesignals 22 aktiviert wird. Das vom Empfänger 10 empfangene Antwortcodesignal 22 wird nun wiederum im Codevergleicher 12 mit dem in den Lesespeicher 11 eingeschriebenen Zufallscodesignal 20 verglichen und — da die beiden Signale 22 und 20 nicht identisch sind bzw. sein müssen — vom Datenauswerter 13 verarbeitet, welcher bei Bestätigung der beiden Codesignale 22 und 20 ein Signal 23 zur Entriegelung des Schlosses 17 abgibt.

Hat nun ein Unbefugter den gesamten Dialog zwischen elektronischem Schlüssel 2 und Schloßsteuerung 3 aufgezeichnet, also die Signale 18, 20 und 22, so führt die Benutzung dieser Aufzeichnung trotzdem nicht zur Erzeugung des Signals 23 zum Entriegeln des Schlosses 17, da bei jeder Abgabe des Öffnungscodesignals 18 ein anderes Zufallscodesignal 20 und Antwortcodesignal 22 erzeugt wird. Selbst eine mehrfache Benutzung des aufgezeichneten Dialoges durch den Unbefugten führt nicht zu einer zufälligen Erzeugung des Signals 23, da in einer weiteren Ausgestaltung des Erfindungsgegenstandes als weitere Sicherheitsvorkehrung in dem elektronischen Baustein 9 der Schloßsteuerung 3 noch ein Zähler- und Zeitschalter 14 vorgesehen sein kann, welcher zum einen bewirken kann, daß er bei fehlendem oder falschem Antwortcodesignal 22 vom Datenauswerter 13 aktiviert wird und das Schaltsignal zur erneuten Abgabe von Fragecode 19 aus dem Speicher 11 nur mit erheblicher Verzögerung weitergibt und zum anderen bewirken kann, daß er bei häufigen Öffnungscodesignalempfängen innerhalb einer kurzen Zeiteinheit aktiviert wird und seinerseits ein Verweigerungsglied 15 aktiviert, welches die Abgabe von Fragecode 19 verhindert. Ein aktiviertes Verweigerungsglied 15 gestattet es auch dem Eigentümer nicht mehr, über den normalen Dialog das Schloß zu entriegeln. Es ist für ihn dann ein sicheres Indiz dafür, daß von Unbefugten versucht wurde, die Tür zu öffnen. Um jedoch den Eigentümer in die Lage zu versetzen, über den normalen Dialog die Tür wieder öffnen zu können, ist in dem Speicher 5 des elektronischen Schlüssels 2 ein zusätzlicher Code gespeichert, welcher durch eine besondere Taste am Sender 4 als separates Entsperrcodesignal 24 ausgesendet und unmittelbar am Empfänger 10 der Schloßsteuerung 3 abgegeben zu einer Inaktivierung des Verweigerungsgliedes 15 führt.

Hierzu 1 Blatt Zeichnungen

– Leerseite –

Nummer: 33 13 098
Int. Cl.³: E 05 B 49/00
Veröffentlichungstag: 11. Oktober 1984